Knocking down the HACIENDA with TCP Stealth

Christian Grothoff
Actual work: Julian Kirsch

Technische Universität München

May 8, 2015

What is HACIENDA?

- Data reconnaissance tool developed by the CITD team in JTRIG
- Port Scans entire countries
  - Uses nmap as port scanning tool
  - Uses GEOFUSION for IP Geolocation
  - Randomly scans every IP identified for that country

Countries

- Completed full scans of 27 countries including
  - [redacted]
- Completed partial scans of 5 additional countries

Tasking & Access

- To task HACIENDA with a Country or Subnet
  - [redacted]@gchq.gov.uk)
  - CITD alias ([redacted]@gchq.gov.uk)
- Access to the Data
  - At GCHQ, request a GLOBAL SURGE account from [redacted]@gchq.gov.uk)
  - At CSEC, contact
  - At NSA, contact
  - At DSD, contact

Ports

- Pulls back hostname, banners, application names and port status
- Gathers additional information for…
  - 21 (ftp): directory listing
  - 80 (http): content of main page
  - 443 (https): content of main page
  - 111 (rpc): results of rpcinfo

How is it used?

- CNE
  - ORB Detection
  - Vulnerability Assessments
- SD
  - Network Analysis
  - Target Discovery

Step 3

Hacking in SIGINT

The Hacking Process

1. (**R**)econnaissance
2. (**I**)nfection
3. (**C**)ommand And Control
4. (**E**)xfiltration

Reconnaissance

Publicly Available Information

(Email Address, Location, Network Info, Passwords, etc.)

Research

Hacker

Victim

Enumerate (Network)

Scan (Services)

Operating Systems

Versions

Domain Names

Reconnaissance Infection Command and Control Exfiltration

Reconnaissance

This system is audited for USSID 18 and Human Rights Act compliance
CLASSIFICATION: TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

X-KEYSCORE C2C Session Viewer

Session 1 of 4

Datetime	Case Notation	From IP	To IP	From Port	To Port	Protocol
2012-05-16 13:03:20	2CBAB00000M0210	[redacted]		01701	01701	icmp

Session | Header (3) | Meta (7) | GENESIS Contexts (1)

Formatter: WIRESHARK | Send to: Download Session | Mode: Snippet | Options | Search Content: Enter text to search

Quick Clicks

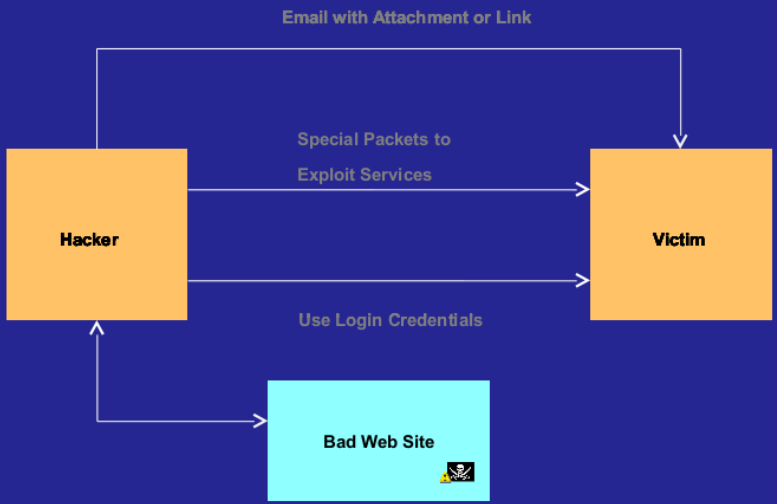
- Session
- One-Click Searches
  - Find fingerprint
    - selector/cadence/task_
    - udp/tunnel/ipv4
    - netmanagement/icmp/s
  - Find traffic on
  - Find application
    - netmanagement/icmp

```
Internet Protocol, Src: 8.8.8.8 (8.8.8.8), Dst: 192.168.0.83 (192.168.0.83)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 60
    Identification: 0x2d3c (11580)
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 51
    Protocol: ICMP (0x01)
    Header checksum: 0x897a [correct]
        [Good: True]
        [Bad : False]
    Source: 8.8.8.8 (8.8.8.8)
    Destination: 192.168.0.83 (192.168.0.83)
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0 ()
    Checksum: 0x52ec [correct]
    Identifier: 0x0001
    Sequence number: 623 (0x026f)
    Data (32 bytes)

0000  61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70   abcdefghijklmnop
0010  71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69   qrstuvwabcdefghi
```

Reconnaissance Infection Command and Control Exfiltration

Infection



Reconnaissance Infection Command and Control Exfiltration

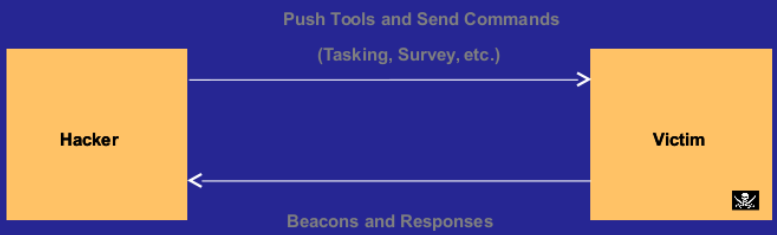
Password Guessing

```
USER Administrator
PASS #mafiavafute197532@%!?*
USER Administrator
PASS sh3l5l1k3p4rty3v3r
USER Administrator
PASS Sh3I5Lik3P4rtY@v3r
USER Administrator
PASS Sh5I8LiK6P8rtY6v5r
USER Administrator
PASS kalimero4cappy
USER Administrator
PASS P@ssword
USER Administrator
PASS P@sswOrd
USER Administrator
PASS P@sswOrd
```

Iraqi Ministry of Finance

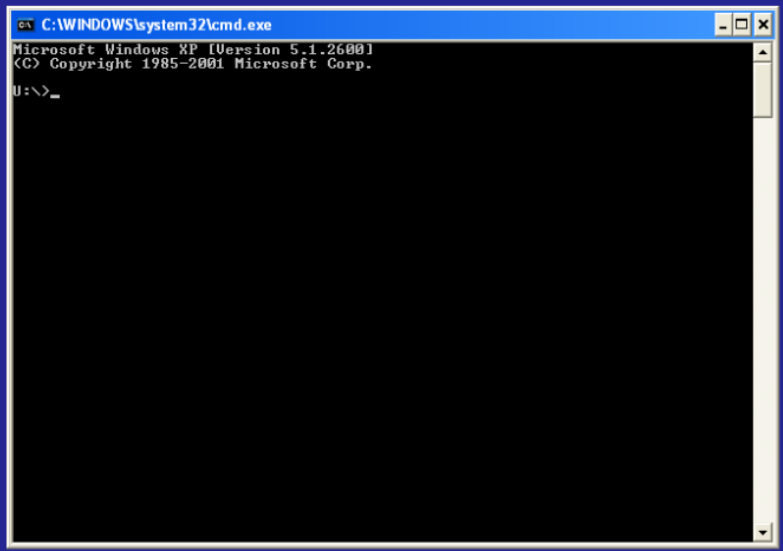
Reconnaissance Infection Command and Control Exfiltration

Command and Control



Reconnaissance Infection **Command and Control** Exfiltration

Windows cmd.exe



Reconnaissance Infection **Command and Control** Exfiltration

Exfiltration

Exfil using known and custom protocols

(Known: HTTP, SMTP, ICMP, FTP, etc)

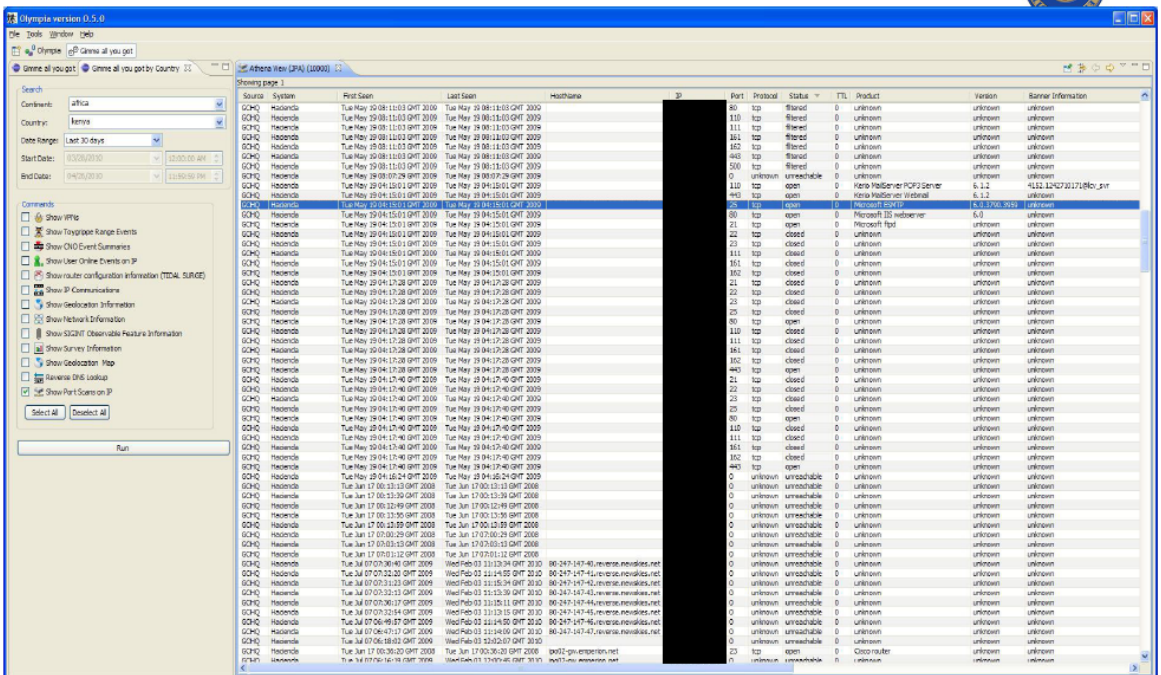
Reconnaissance Infection Command and Control Exfiltration

How is it used?

- CNE
  - ORB Detection
  - Vulnerability Assessments
- SD
  - Network Analysis
  - Target Discovery

LANDMARK

- CSEC's Operational Relay Box (ORB) covert infrastructure used to provide an additional level of non-attribution; subsequently used for exploits and exfiltration
- 2-3 times/year, 1 day focused effort to acquire as many new ORBs as possible in as many non 5-Eyes countries as possible



BUT, network analysis still manual!

[redacted]

- [redacted] GSM provider
- NSA TAO requested assistance gaining access to the network
- Network analysis using OLYMPIA:
  - DNS query to determine IP address
  - IP address to network range
  - Network range to port scan
  - Are there any vulnerable devices in that range?
- Duration: < 5 minutes

MUGSHOT GOALS

- Automated Target Characterisation and Monitoring
  - Automatically understand everything **important** about **CNE target networks** from passive and active sources.
- Automated Un-Targeted Characterisation
  - Automatically understand everything **important** about **all machines** on the Internet from passive and active sources.

[redacted]

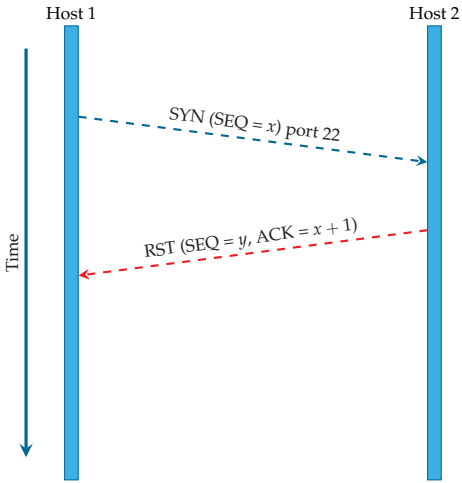
So, is it all lost?

Two Solutions

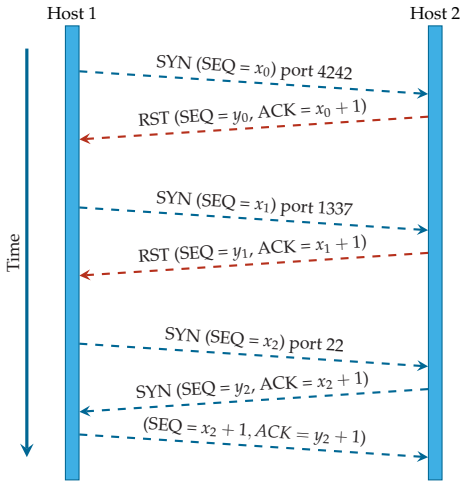
- Backwards-compatible minimally invasive hotfix
- Clean-slate principled rearchitecture

An Introduction to Port Knocking

No knock, no fun

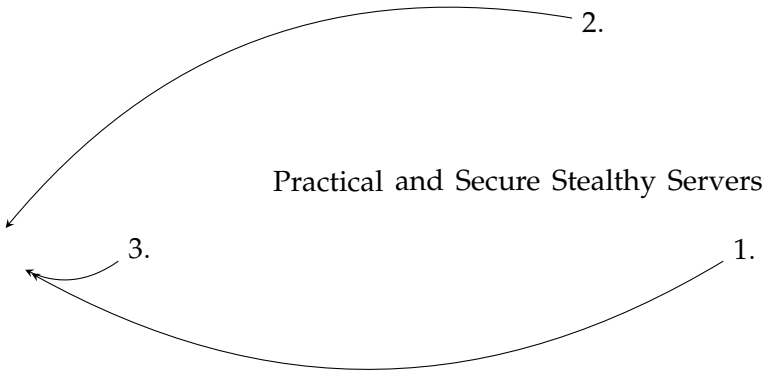


Port knocking example



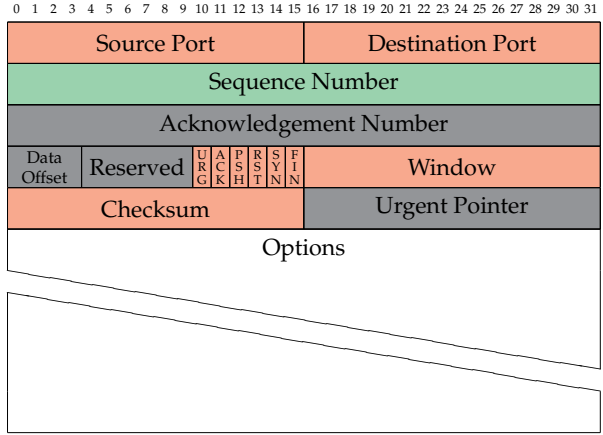
Design

Overview



Design

Stealthiness



Design (v1)

Security

- Destination IP address IP_d
- Destination port P_d
- TCP timestamp T
- Pre-Shared Key S
- Hash function h

Authentication Security Token (AV)

$\text{AV} := h((IP_d, P_d, T), S)$

- ISN := AV

SECONDDATE

- SECONDDATE is an exploitation technique that takes advantage of web-based protocols and man-in-the-middle (MitM) positioning.
- SECONDDATE influences real-time communications between client and server and can quietly redirect web-browsers to FA servers for individual client exploitation.
- This allows mass exploitation potential for clients passing through network choke points, but is configurable to provide surgical target selection as well.

Design (v2)
Security

- Destination IP address IP_d
- Destination port P_d
- TCP timestamp T
- Pre-Shared Key S
- Hash functions h, h'
- Payload p

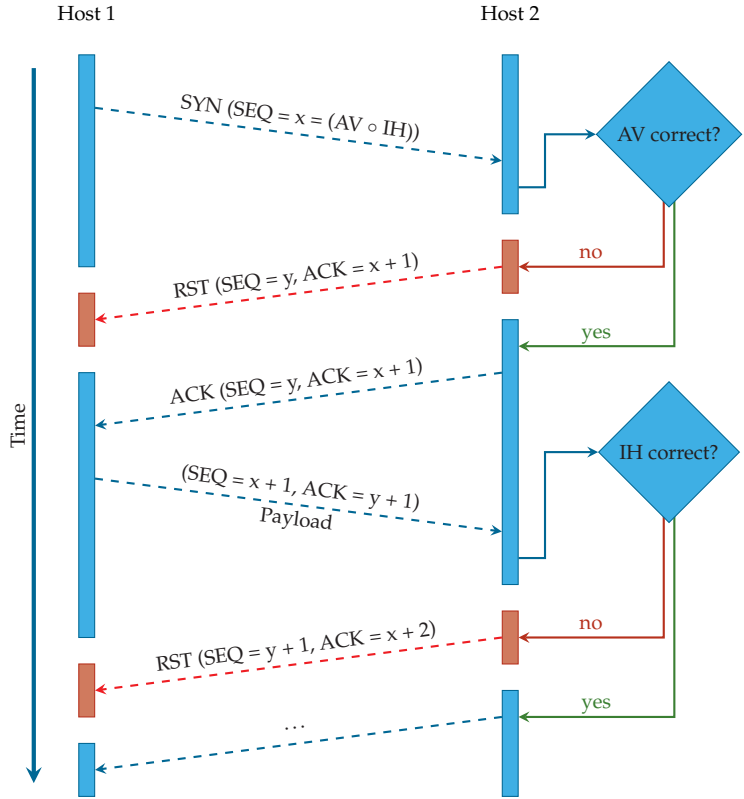
TCP Payload Integrity Protector IH

$\text{IH} := h'(S \circ p)$

Authentication Security Token AV

$\text{AV} := h((IP_d, P_d, T, \text{IH}), S)$

- $\text{ISN} := \text{AV} \circ \text{IH}$


Host 1
Host 2
Time
SYN (SEQ = x = (AV ∘ IH))
AV correct?
no
RST (SEQ = y, ACK = x + 1)
yes
ACK (SEQ = y, ACK = x + 1)
IH correct?
(SEQ = x + 1, ACK = y + 1)
Payload
no
RST (SEQ = y + 1, ACK = x + 2)
yes
…

Design
Ease of Use

- Source IP and Port *not* included in ISN generation
  $\Rightarrow$ Compatibility with NATs
- Knocking is implemented *in the kernel*
  $\Rightarrow$ No fiddling with config-files, firewall rules or daemons
  $\Rightarrow$ Trivial to use from an application developer's perspective

Design

Ease of Use – TCP Stealth Server

```
1  char secret[64] = "This is my magic ID.";
2  int payload_len = 4;
3  int sock;
4
5  sock = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP);
6  if (sock < 0) {
7          printf("socket() failed, %s\n", strerror(errno));
8          return 1;
9  }
10 if (setsockopt(sock, IPPROTO_TCP, TCP_STEALTH, secret, sizeof(secret))) {
11         printf("setsockopt() failed, %s\n", strerror(errno));
12         return 1;
13 }
14 if (setsockopt(sock, IPPROTO_TCP, TCP_STEALTH_INTEGRITY_LEN,
15                &payload_len, sizeof(payload_len))) {
16         printf("setsockopt() failed, %s\n", strerror(errno));
17         return 1;
18 }
19 /* Continue with bind(), listen(), accept(), recv(), ... */
```

Design

Ease of Use – TCP Stealth Client

```
1  char secret[64] = "This is my magic ID.";
2  char payload[4] = "1234";
3  int sock;
4
5  sock = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP);
6  if (sock < 0) {
7          printf("socket() failed, %s\n", strerror(errno));
8          return 1;
9  }
10 if (setsockopt(sock, IPPROTO_TCP, TCP_STEALTH, secret, sizeof(secret))) {
11         printf("setsockopt() failed, %s\n", strerror(errno));
12         return 1;
13 }
14 if (setsockopt(sock, IPPROTO_TCP, TCP_STEALTH_INTEGRITY,
15                payload, sizeof(payload))) {
16         printf("setsockopt() failed, %s\n", strerror(errno));
17         return 1;
18 }
19 /* Continue with connect(), send(), ... */
```

Design

Ease of Use – libknockify

- Shared library for use at compile- or run-time
- Enables TCP Stealth functionality for legacy code

```
$ LD_PRELOAD=./libknockify.so ncat knock-server application-port
```

- Configuration options (such as the TCP Stealth secret) are given as environment variables or via a special file

Limitations

- Distribution of the Pre-Shared Key
- ISN has only 32 bits

Limitations

- Distribution of the Pre-Shared Key
- ISN has only 32 bits
- Changes to ISN and TSVal by middle boxes:

	TCP Port		
Behavior	34343	80	443
Unchanged	**126 (93%)**	116 (82%)	128 (90%)
Mod. outbound	5 (4%)	5 (4%)	6 (4%)
Mod. inbound	0 (0%)	1 (1%)	1 (1%)
Mod. both	4 (3%)	13 (9%)	7 (5%)
Proxy (probably mod. both)	0 (0%)	7 (5%)	0 (0%)
Total	135 (100%)	142 (100%)	142 (100%)

Numbers by Honda et al. “Is it Still Possible to Extend TCP?”

Limitations

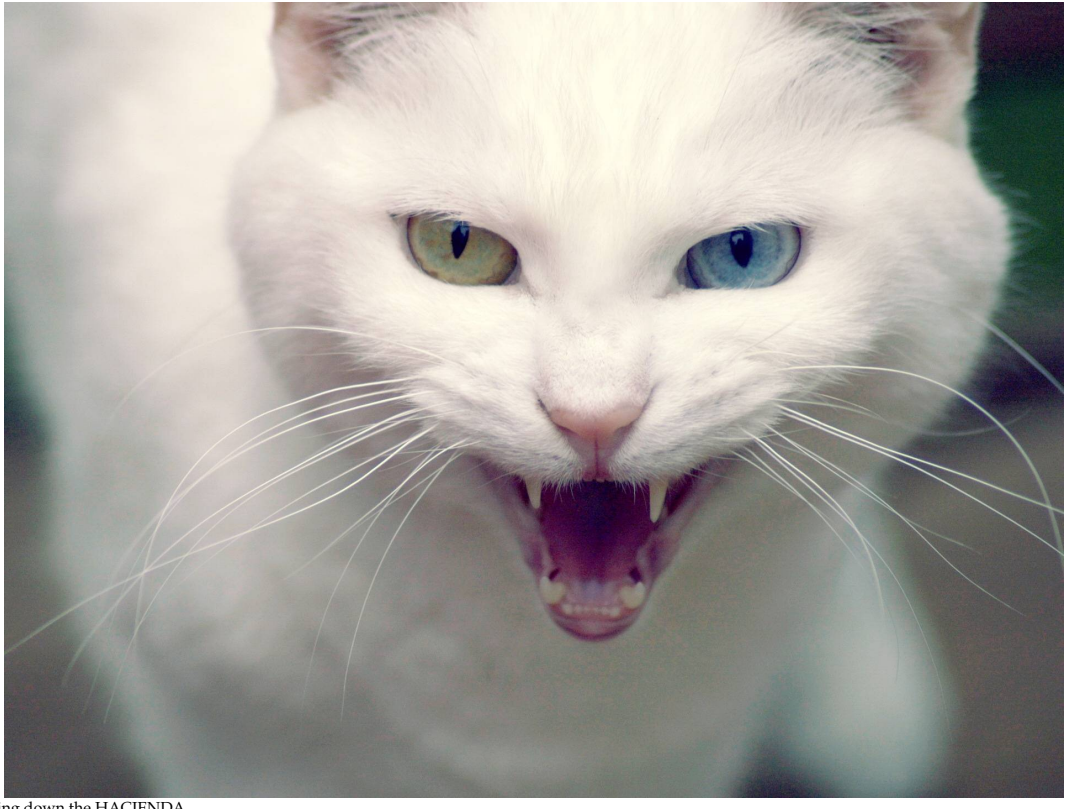
- Distribution of the Pre-Shared Key
- ISN has only 32 bits
- Changes to ISN and TSVal by middle boxes:

	TCP Port		
Behavior	34343	80	443
Unchanged	**126 (93%)**	116 (82%)	128 (90%)
Mod. outbound	5 (4%)	5 (4%)	6 (4%)
Mod. inbound	0 (0%)	1 (1%)	1 (1%)
Mod. both	4 (3%)	13 (9%)	7 (5%)
Proxy (probably mod. both)	0 (0%)	7 (5%)	0 (0%)
Total	135 (100%)	142 (100%)	142 (100%)

Numbers by Honda et al. “Is it Still Possible to Extend TCP?”

- IETF, Linux and FreeBSD communities so far fail to adopt

Cat break (sponsored by IRTF)



HACIENDA is a **port** *mapper*.

HACIENDA is a **port** *mapper*.

What else does the NSA *map*?

HACIENDA is a **port** *mapper*.

What else does the NSA *map*?

Let's ask The Intercept...

(U) What is TREASUREMAP?

(U//FOUO) Capability for building a near real-time, interactive map of the global internet.

Map the entire Internet – Any device*, anywhere, all the time

(U//FOUO) We enable a wide range of missions:

- Cyber Situational Awareness – *your own network plus adversaries'*
- Common Operation Pictures (COP)
- Computer Attack/Exploit Planning / Preparation of the Environment
- Network Reconnaissance
- Measures of Effectiveness (MOE)

(* limited only by available data)

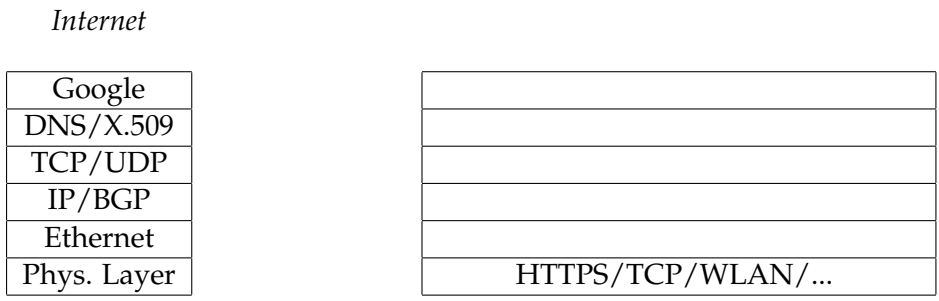
Time to Build a ~~NEW~~GNU Network

The ~~NEW~~GNU Network (very simplified)

Internet

Google
DNS/X.509
TCP/UDP
IP/BGP
Ethernet
Phys. Layer

The ~~NEW~~GNU Network (very simplified)



The ~~NEW~~GNU Network (very simplified)

Internet

Google
DNS/X.509
TCP/UDP
IP/BGP
Ethernet
Phys. Layer

CORE (OTR)
HTTPS/TCP/WLAN/...

The ~~NEW~~GNU Network (very simplified)

Internet

Google
DNS/X.509
TCP/UDP
IP/BGP
Ethernet
Phys. Layer

R^5N DHT (KBR)
CORE (OTR)
HTTPS/TCP/WLAN/...

The ~~NEW~~GNU Network (very simplified)

Internet

Google
DNS/X.509
TCP/UDP
IP/BGP
Ethernet
Phys. Layer

CADET (SCTP+Axolotl+TCP Stealth)
R^5N DHT (KBR)
CORE (OTR)
HTTPS/TCP/WLAN/...

The ~~NEW~~GNU Network (very simplified)

Internet

Google
DNS/X.509
TCP/UDP
IP/BGP
Ethernet
Phys. Layer

GNU Name System
CADET (SCTP+Axolotl+TCP Stealth)
R^5N DHT (KBR)
CORE (OTR)
HTTPS/TCP/WLAN/...

The ~~NEW~~GNU Network (very simplified)

Internet

Google
DNS/X.509
TCP/UDP
IP/BGP
Ethernet
Phys. Layer

Applications
GNU Name System
CADET (SCTP+Axolotl+TCP Stealth)
R^5N DHT (KBR)
CORE (OTR)
HTTPS/TCP/WLAN/...

The ~~NEW~~GNU Network (very simplified)

Internet

Google
DNS/X.509
TCP/UDP
IP/BGP
Ethernet
Phys. Layer

GNUnet

Applications
GNU Name System
CADET (SCTP+Axolotl+TCP Stealth)
R^5N DHT (KBR)
CORE (OTR)
HTTPS/TCP/WLAN/...

Limitations

- ~~Distribution of the Pre-Shared Key~~ — use GNU Name System

Limitations

- ~~Distribution of the Pre-Shared Key~~ — use GNU Name System
- ~~ISN has only 32 bits~~ — use 256 bits

Limitations

- ~~Distribution of the Pre-Shared Key~~ — use GNU Name System
- ~~ISN has only 32 bits~~ — use 256 bits
- ~~Changes to ISN and TSVal by middle boxes~~ — irrelevant in overlay

Limitations

- ~~Distribution of the Pre-Shared Key~~ — use GNU Name System
- ~~ISN has only 32 bits~~ — use 256 bits
- ~~Changes to ISN and TSVal by middle boxes~~ — irrelevant in overlay
- ~~IETF, Linux and FreeBSD communities so far fail to adopt~~ — all in userspace

Limitations

- ~~Distribution of the Pre-Shared Key~~ — use GNU Name System
- ~~ISN has only 32 bits~~ — use 256 bits
- ~~Changes to ISN and TSVal by middle boxes~~ — irrelevant in overlay
- ~~IETF, Linux and FreeBSD communities so far fail to adopt~~ — all in userspace
- More issues to address $\Rightarrow$ more research! (not done yet!)

A Pattern of Hope

Spy Program	Target	Defense	Started
FTM/TRACFIN	SWIFT/VISA/etc.	DigiCash/GNU Taler	1990
TREASUREMAP	Internet (all)	Freenet/GNUnet/Tor	2000
HACIENDA	vuln. TCP service	Port Knocking	2000
BULLRUN/DUAL_EC_DRBG	PRNG (backdoor)	n/a	2004
BULLRUN/LONGHAUL	TLS/IPSEC (keys)	OTR/AXOLOTL	2004
MJOLNIR	Long-path in Tor	Tor 0.2.3.11	2007
PRISM	US big data corps	SecuShare	2009
MORECOWBELL	DNS	GNU Name System	2012
...	...	...	...

Questions?

Find more information at:

- https://gnunet.org/
- https://gnunet.org/knock
- https://gnunet.org/gns
- https://gnunet.org/mcb
- http://www.taler.net/

Thanks to:
Julian Kirsch
Jacob Appelbaum
Monika Ermert
Laura Poitras
Henrik Moltke
Maurice Leclaire
Andreas Enge
Bart Polot
Luca Saiu
The Source

This work was funded by the Deutsche Forschungsgemeinschaft (DFG) under ENP GR 3688/1-1.

Slides will be at http://grothoff.org/christian/.

Limitations

RFC 1323: TCP Extensions for High Performance